IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 3, Ver. II (May - June 2017), PP 23-30
www.iosrjournals.org

A Privacy Preserving Scheme for Data Security in the Video Surveillance

Swati K. Kulkarni[1], Akshata A. Raut[2], Vibha V. Walekar[3]
Department of Electronics and Telecommunication Engineering MGM College of Engineering and Technology, Navi Mumbai, India.

***Abstract**: This paper proposes a privacy preserving scheme for data security in the video surveillance. Nowadays, significant concerns about human privacy have been growing along with the extensive application of surveillance cameras. Successful automated video surveillance services are expected to provide effective means for enhancing the individual's privacy protection. Recently, many studies about privacy protection in video surveillance have been proposed. Clearly, for video surveillance, privacy protection can be carried out before or after the video compression. Actually, for the videos captured by cameras, many compression standards have been developed, like H.120, H.261, MPEG-1, H.263 and H.264. The system is stable, reasonable and reliable.*

***Keywords**: Data Security; Quantum cryptography; Video surveillance; Video Encryption; Chaos Algorithm; Wireless communication.*

I. Introduction

Today's video surveillance system is widely used in our daily life due to the various problems are going on in the society such as bank robbery, crimes, murder, terrorist attacks etc. Images and videos are easily leaked because traditional encryption methods are easily cracked. For security, reducing loss and theft, real time remote monitoring service, improving productivity, video surveillance system is useful. It is important to monitored all things but which is not seen by third person [1]. To get more security and bandwidth, we used quantum cryptography technology. For better coding efficiency, video compression technologies using hybrid approach is used [2]. The quantum cryptography allows completion of various cryptographic tasks which are impossible using classical communication. Quantum cryptography uses photons or particles to generate and transmit key. The key is received at the receiver using communication channel [3]. The information carrier is nothing but entangled photon pairs which are used to keep transmission of video information confidential [4]. Here the communication channel is optical fibre network which provides faster transmission of data.

II. Proposed System

The overall system comprises of an image capturing system which captures the individual frame of images which is shown in figure 1. The paper intends to use our personal computer as a medium for processing the video data, compression and encryption of video data and will be using MATLAB and C# for the same, and once the compression and encryption is completed it is transmitted to the receiver end using serial to optical converter and optical to serial converter. The key transmission occurs through the medium of an optical fiber using photons which is quantum cryptography and that happens to be our principle concept which we have implemented. The detail components of hardware structure of system are shown in figure 2.

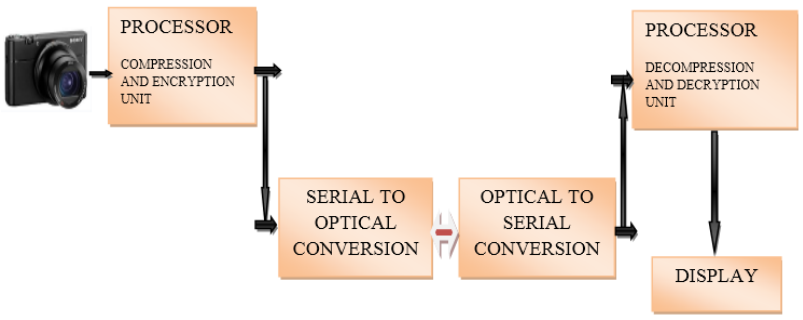


Figure 1. Proposed system

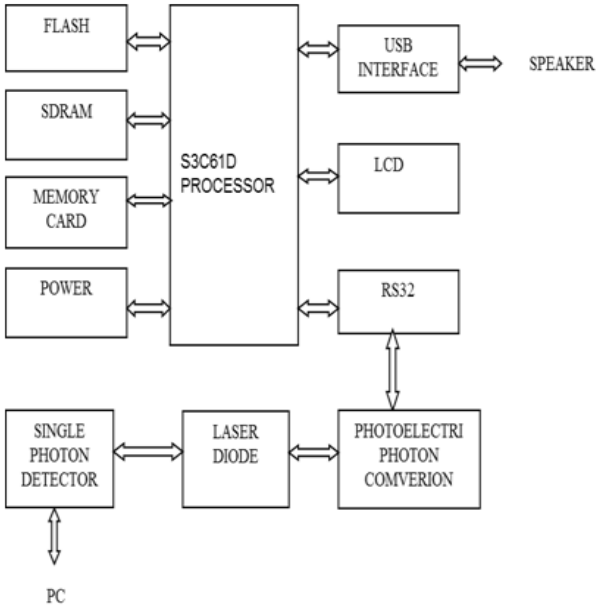


Figure 2. Hardware structure of system

A. Compression:

The initial step of compression involves:-

i. Fetching single frame from the video.
ii. Once the frame is fetched we need to fetch the first pixel.
iii. Out of the 8 bits pixels we discard the last 4 bits
iv. Thus generating the compressed image.
v. Now by doing this, the data held by 2 pixels is represented as one pixel which leaded to overall compression.

B. Encryption:

Once compression is performed on the image, we shift or rotate it by 4 bits i.e. If we have a pixel 1101 1001 we would get 1001 1101 after rotating it by 4 bits. This is how encryption is performed on the video data.

C. Decryption*:*

For decryption of data at the receiver end we fetch the individual pixel of the concerned frame and then we shift or rotate the bits by 4 bits in a manner similar to that in the process of encryption.

D. Decompression*:*

The step of decompression involves:-

i. Both the processes go hand in hand, once decryption is performed on pixel of the concerned frame.
ii. We decompress the image by adding 0000.
iii. After every four bits thus 1101 1001 would be represented by 1101 0000 and 1001 0000.
iv. Thus we obtain the decompressed image but the obtained image is comparatively lighter.

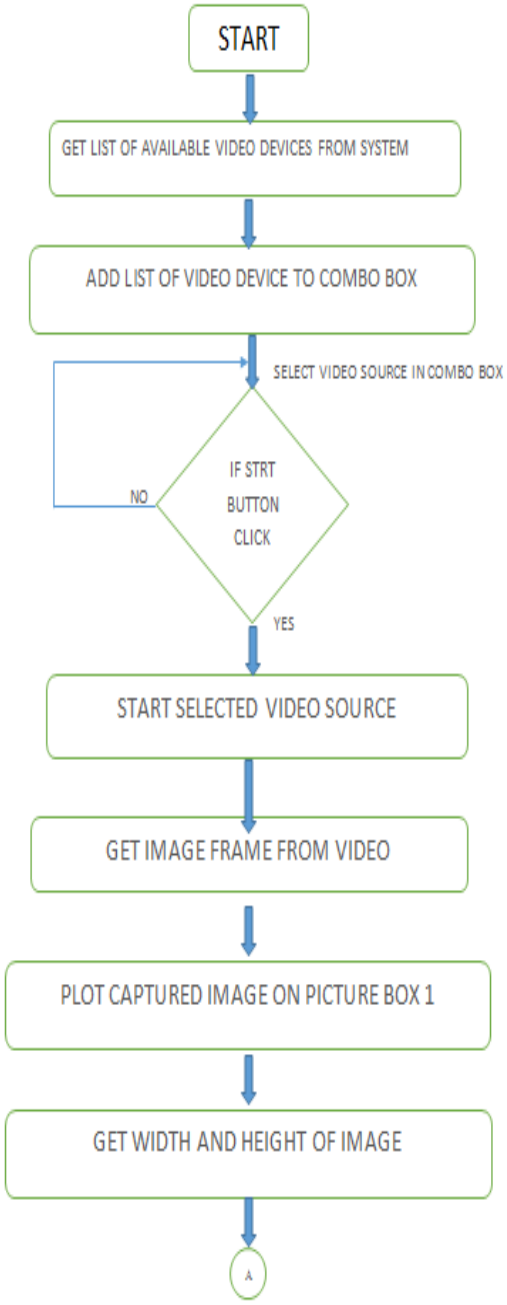
E. Quantum cryptography:

Quantum cryptography is NOT a new algorithm to encrypt and decrypt data. Rather it is a technique of using photons to generate a cryptographic key and transmit it to a receiver using a suitable communication channel. A cryptographic key plays the most important role in cryptography; it is used to encrypt/decrypt data. Essentially, quantum cryptography is based on the usage of individual particles/waves of light (photon). It is also based on their intrinsic quantum properties to develop an unbreakable cryptosystem. They are the information carriers in optical fiber cables, the most promising medium for extremely high-bandwidth communications [3]. The idea behind quantum cryptography is that two people communicating using a quantum channel can be absolutely sure no one is eavesdropping. No disturbance, no eavesdropper. In simple word quantum cryptography is completely secure. Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a key. The paper is associated with data to a photon by associating binary bits 1 and 0 to the

glow on and off of the Infrared LED. When the LED glows the receiver led considers it as binary 1 and when the led stays off it is considered as binary 0 which is how the key is represented. Thus successful transmission of key occurs. Quantum Key Distribution (QKD) is a technology to generate and distribute provably secure cipher keys over unsecured channels. It does this using single photon technology and can detect potential eavesdropping via the quantum bit error rates of the quantum channel. Sending randomly encoded information on single photons produces a shared secret that is a random string and the probabilistic nature of measuring the photon state provides the basis of its security [5].

III. Flowchart

Figure 3 shows Flowchart of the system which gives the overview about the program.



This gives detailed information about system flow chart and programs which are used by the microcontroller for initializing, processing and transmitting information

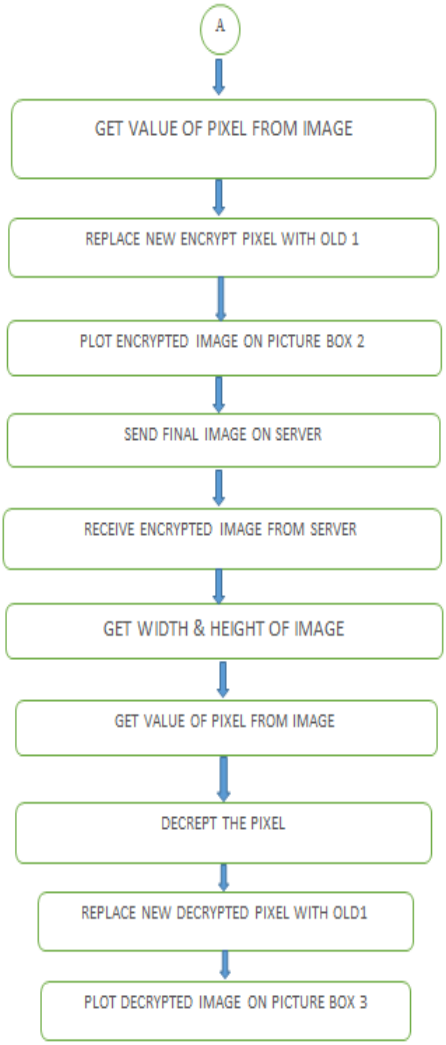


Figure3. Flowchart of the program

Encryption Algorithm:

The encryption algorithm that is being used in the project is commonly known as 'Chaos'. The initial step is to fetch the individual pixel from the image and we perform compression on it by discarding the last 4 bits of the pixel. Thus 2 pixels are equivalent to one pixel. This is done by using AND operation on the pixel i.e. AND it with 11110000. Then addition of 2 pixels is performed on which compression is performed. Once it is done the bits are shifted or rotated by 4, thus the entire value of pixel changes thus encryption is successfully performed.

Example:

Pixel 1(p1) = 234(decimal) → EA (hexadecimal)

↓

11101010(binary)

Pixel 2(p2) = 125(decimal) → 7D (hexadecimal)

↓

01111101(binary)

Performing AND operation

p1 → 11101010 AND 11110000 p1 =11100000

p2 → 01111101 AND 11110000 p2 =01110000

Let p1 equal to p3.

p3 → p1 p3 =11100000

Shifting p2 towards left by 4 bit

p4 → p2 >>4 p4 = 00000111

p5 → p3+p4 p5 = 11100111

Asynchronous Video Transfer:

The concept of asynchronous streaming is to perform the asynchronous streaming task, where it will revert to the class that is in the Push Stream Content. It allows the developer to progressively push packets of data down to the receiving client. Then it will read the video stream from the file on the server's hard drive, and flush it down to the client (using Push Stream Content) in the packets of 65,536 bytes. The streaming video playback could then start immediately (client doesn't have to wait for the entire video to be flushed down), without causing unnecessary load on the server, especially as the process of writing to the client happens asynchronously. Once the client disconnects the writing stops. This Action is called as soon as the output stream (HTTP content to be flushed to the client) becomes available. Therefore, we could create a small helper class, which would read the from the disk, and expose this activity for PushStreamContent to call repeatedly. It allows the consumer of the class to give as information about the file (for which we arbitrarily look in a specific location, the Downloads folder in this case). In the WriteToStream method, it proceeds to read the file progressively and flush these bits to the output stream. Notice that the signature of this method matches the Action expected by PushStreamContent and as a result can be used by it. Now the controller action, will allow the client to pass video info (name, extension), construct the instance of VideoStream and then create an instance of PushStreamContent which gets returned to the client. This is how live video streaming is established.

IV. Simulation And Results

Figure 4 shows circuit simulation layout in Proteus professional 8.

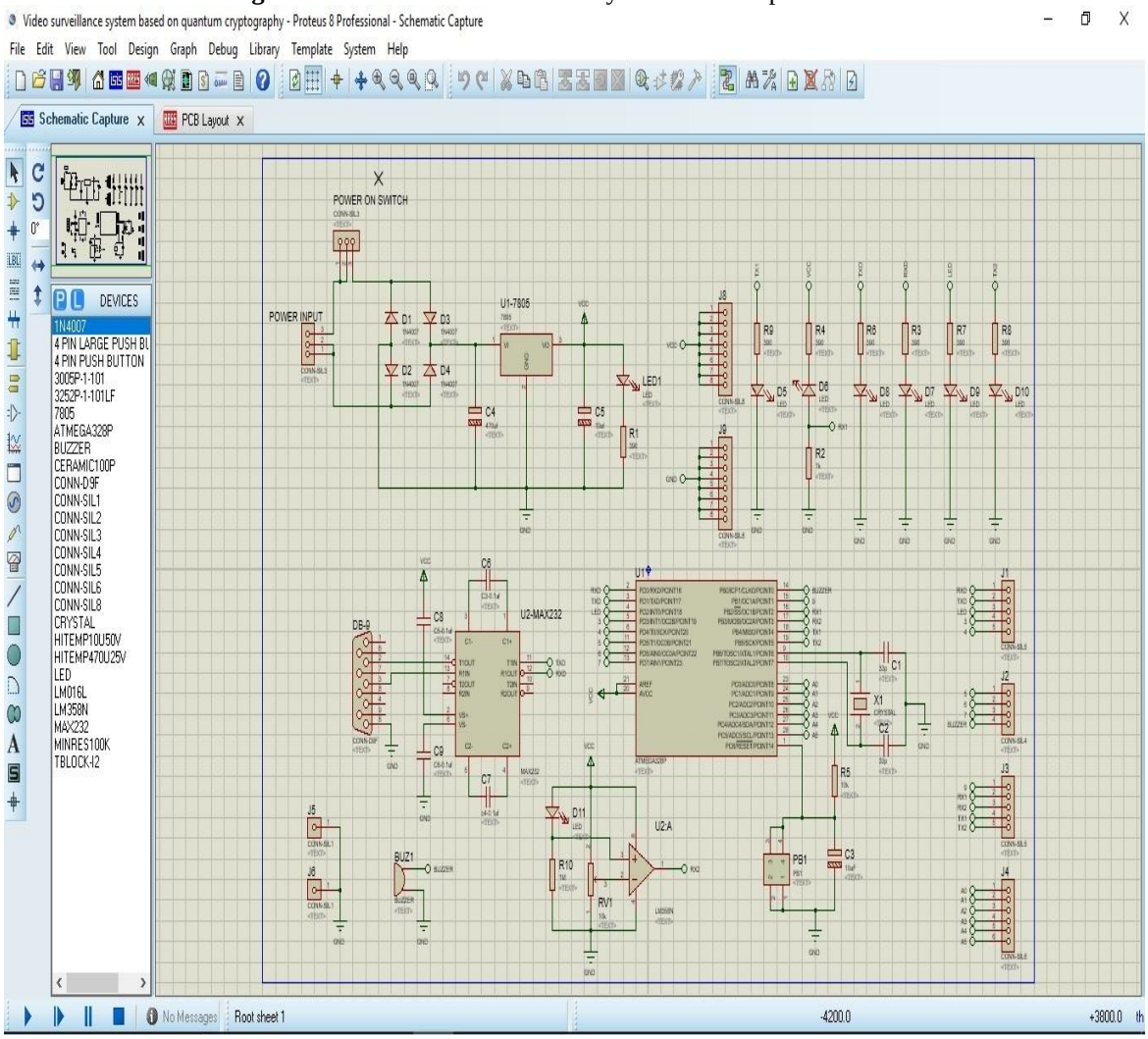


Figure 4. Circuit simulation layout in Proteus

Figure 5 shows coding window which contain all codes.

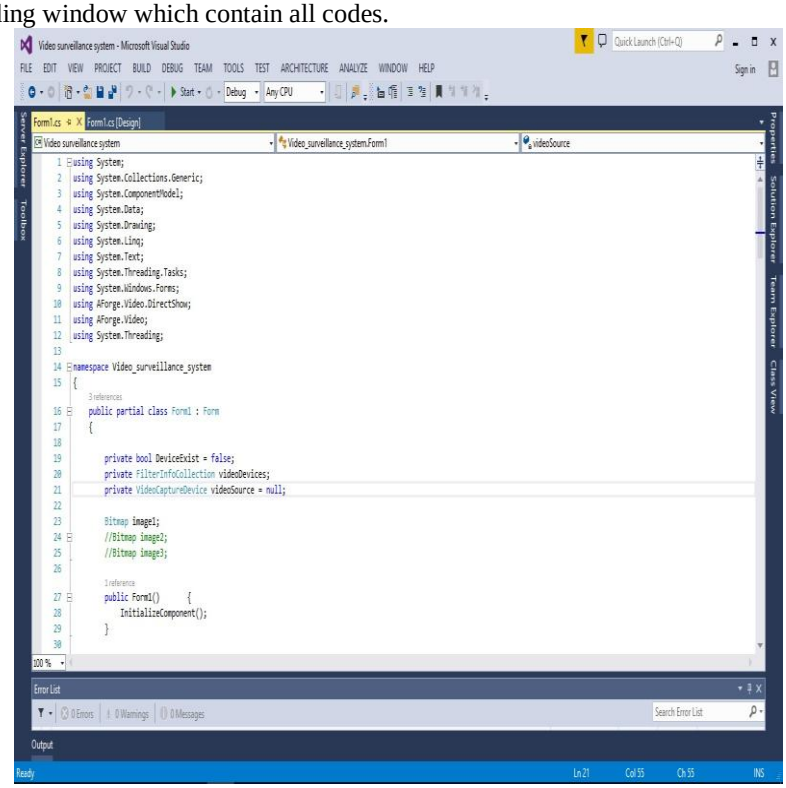


Figure 5. *Coding window*

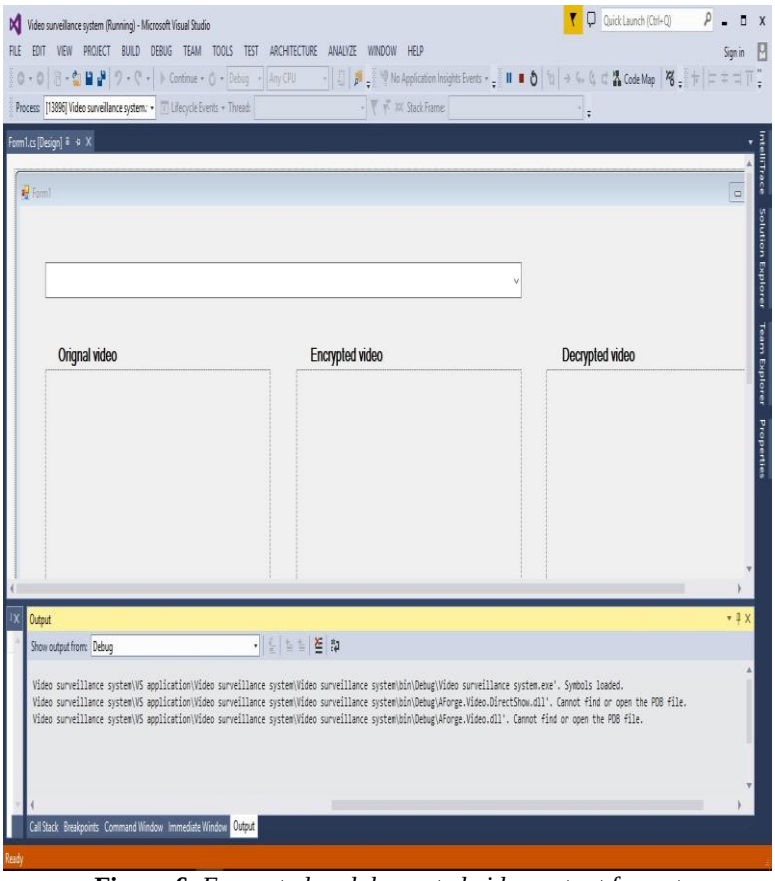


Figure 6. *Encrypted and decrypted video output format*

Figure 6 shows original video format and encrypted & decrypted video output format.
Figure 7 shows original video and its result of encrypted and decrypted video.

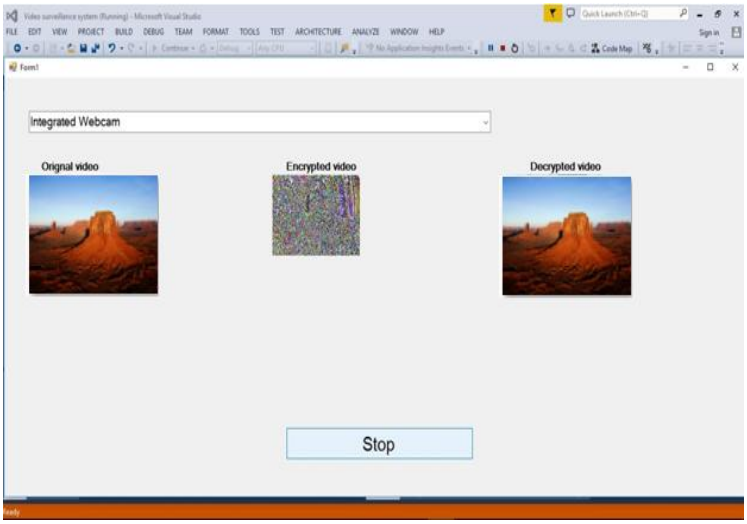


Figure 7. Encrypted and decrypted video result

V. Conclusion

Privacy and data security is right now of utmost importance to people. With quantum cryptography, secure transmission of data is possible, and chances of confidential data being intercepted and altered are very low. This technology has been implemented in some areas. But it is still under deeper research before being widely implemented. With upcoming future proof projects there is a need for a futuristic technology that matches up to the standards that are required for growth of humankind and quantum cryptography is a perfect solution for that, basically it can be implemented in every project that involves a real time visual data capture. The video stream is extremely important source of information and needs to be protected and we need efficient measures for protecting the same. This system eventually achieves the stability and good image quality, higher inter frame compression and video acquisition system. Thus quantum cryptography is an ideal solution for such applications.

VI. Future Scope

With growing threats we need to have newer advanced method to cope up with these threats and quantum cryptography seems to be a perfect replacement for the existing outdated system which are already exposed to so many threats. With increasing research on quantum computers interfacing the two technologies could give us a full proof system.

i. Video calling – it could be used for end to end encryption while using it for real time interactive applications such as WhatsApp video calling or Skype video calling.
ii. Military drones –video captured by the military drones can be safeguarded using this technique wherein the video can be decrypted once they receive the key from the photon stream.
iii. Robotics/land rovers /mars rover – capturing live video using rovers can secure using quantum cryptography.
iv. Self-driving cars which are an upcoming mega project which is based on artificial intelligence, where in we are using a driverless car. The overall system uses wide range of sensors and image processing for recognizing the obstructions or humans and thus it is of utmost importance that the video data doesn't get hacked or tampered.

References

[1] G.Brassard, F.Bussières, N.Godbout and S.Lacroix, "Multiuser quantum key distribution using wavelength division multiplexing," in Proceedings of SPIE 5260:Applications of Photonic Technology 6, Page(s):149–153 (2003).
[2] Chenchou Huang, HsuFeng Hsiao, "Perceptual rate distortion optimization for block mode selection in hybrid video coding," in IEEE Conference Publications, Page(s):489-492 (2013).
[3] K. Sato, B.L. Evans, and J.K. Aggarwal, "Designing an Embedded Video Processing Camera Using a 16-bit Microprocessor for Surveillance System," in Intemational Workshop on Digital and Computational video, Clearwater, FL, Page(s):151-158, November (2002).
[4] Petri Mahonen, "Wireless Video Surveillance: System Concepts," in Proc. Int. Conf. on Image Analysis and Processing, Page(s):1090-1095, Sep. (1999).
[5] Damian Grzechca, Tomasz Wróbel, Patryk Bielecki. "Indoor location and idetification of objects with video survillance system and WiFi module" in Faculty of Automatic Control, Electronics and Computer Science Silesian University of Technolgy Gliwice, Poland, Page(s):171–174 (2014).
[6] Ce Zhu, Bing Xiong, "Transform-Exempted Calculation of Sum of Absolute Hadamard Transformed Differences" in ieee transactions on circuits and systems for video technology, vol. 19, no. 8, page(s):1183–1188 august (2009).

[7] Francesco Ziliani and Andrea Cavallaro, "Image Analysis for Video Surveillance Based on Spatial Regularization of a statistical Model-Based Change Detection," in Signal Processing Laboratory, Swiss Federal Institute of Technology, Real-Time Imaging 7, Page(s): 389-399 (2001).
[8] Fernando M. S. Ramos and Filipe M. PatroAcio, "Application of Distributed Platforms in a Video Surveillance System," in University of Aveiro, Dept. of Communication and Art, Page(s): 447-455 (2001).
[9] H. U. Jianmiao and CEN Jianmei, "Video surveillance in public space in China," Page(s): 474–488 (2009).
[10] Cornelius Held, Julia krumm, petra Markel, and Ralf p. Schenke, "Intelligent Video Surveillance" by the IEEE computer society, Page(s): 83-84, March (2012).